Our Ref.: JJVC-146-PCT-US

English translation of Amendment under PCT Article 34

PCT/JP2005/001211

number sequence or transmitted/received data is observed.

[0008]

In order to accomplish the object, a first aspect of the present invention provides a pseudorandom number generator for generating a pseudorandom number sequence of a predetermined bit length, comprising a first linear feedback shift register having **m** steps of shift registers to use a primitive polynomial as a characteristic polynomial thereof, set first initial values and first coefficients to the **m** steps of shift registers, and provide a bit string of a predetermined bit length; a second linear feedback shift register having **n** steps of shift registers to use a characteristic polynomial, set second initial values and second coefficients to the **n** steps of shift registers, and provide a bit string of a predetermined bit length; an initial value generator to generate, according to predetermined conditions, the first and second initial values and supply the first and second initial values respectively to the first linear feedback shift register and second linear feedback shift register; a polynomial coefficient generator to generate, according to predetermined conditions, the second coefficients set to the second linear feedback shift register and supply the second coefficients to the second linear feedback shift register; a primitive polynomial memory to store a plurality of primitive polynomials with identification

information representative of the primitive polynomials, one of the primitive polynomials being used for the first linear feedback shift register; a primitive polynomial selector to select, according to predetermined conditions, one of the primitive polynomials stored in the primitive polynomial memory and supply coefficients of the primitive polynomial as the first coefficients to the first linear feedback shift register; and a pseudorandom number output unit to generate the pseudorandom number sequence of the predetermined bit length by carrying out bit-by-bit logical operations on the bit string provided by the first linear feedback shift register and the bit string provided by the second linear feedback shift register and output the pseudorandom number sequence.

[0009]

According to a second aspect of the present invention that is based on the first aspect, the pseudorandom number generator comprises a communication unit to generate initial data including the identification information of the primitive polynomial selected by the primitive polynomial selector, the first and second initial values generated by the initial value generator, and the second coefficients generated by the polynomial coefficient generator, send the initial data to a second pseudorandom number generator, receive, if any, initial data from the second pseudorandom number generator, extract the first and second initial values

from the received initial data, supply the extracted first and second initial values to the first linear feedback shift register and second linear feedback shift register, extract the second coefficients from the received initial data, supply the extracted second coefficients to the second linear feedback shift register, extract identification information of a primitive polynomial from the received initial data, and supply the extracted identification information to the primitive polynomial selector. The primitive polynomial selector selects one of the primitive polynomials stored in the primitive polynomial memory according to the identification information extracted by the communication unit and supplies coefficients of the primitive polynomial serving as the first coefficients to the first linear feedback shift register.

[0010]

A third aspect of the present invention provides a pseudorandom number generation program for causing a computer to generate a pseudorandom number sequence of a predetermined bit length, the pseudorandom number generation program making the computer function as a first linear feedback shift register having **m** steps of shift registers to use a primitive polynomial as a characteristic polynomial thereof, set first initial values and first coefficients to the **m** steps of shift registers, and provide a bit string of a predetermined

bit length; a second linear feedback shift register having n steps of shift registers to use a characteristic polynomial, set second initial values and second coefficients to the n steps of shift registers, and provide a bit string of a predetermined bit length; initial value generation means for generating, according to predetermined conditions, the first and second initial values and supplying the first and second initial values respectively to the first linear feedback shift register and second linear feedback shift register; polynomial coefficient generation means for generating, according to predetermined conditions, the second coefficients set to the second linear feedback shift register and supplying the second coefficients to the second linear feedback shift register; primitive polynomial memory means for storing a plurality of primitive polynomials with identification information representative of the primitive polynomials, one of the primitive polynomials being used for the first linear feedback shift register; primitive polynomial selection means for selecting, according to predetermined conditions, one of the primitive polynomials stored in the primitive polynomial memory means and supplying coefficients of the primitive polynomial as the first coefficients to the first linear feedback shift register; and pseudorandom number output means for generating the pseudorandom number sequence of the predetermined bit length by carrying out bit-by-bit

logical operations on the bit string provided by the first linear feedback shift register and the bit string provided by the second linear feedback shift register and outputting the pseudorandom number sequence.

[0011]

According to a fourth aspect of the present invention that is based on the third aspect, the pseudorandom number generation program further makes the computer function as communication means for generating initial data including the identification information of the primitive polynomial selected by the primitive polynomial selection means, the first and second initial values generated by the initial value generation means, and the second coefficients generated by the polynomial coefficient generation means, sending the initial data to a second pseudorandom number generator, receiving, if any, initial data from the second pseudorandom number generator, extracting the first and second initial values from the received initial data, supplying the extracted first and second initial values to the first linear feedback shift register and second linear feedback shift register, extracting the second coefficients from the received initial data, supplying the extracted second coefficients to the second linear feedback shift register, extracting identification information of a primitive polynomial from the received initial data, and supplying the extracted identification information to the primitive

polynomial selection means; and the primitive polynomial selection means selects one of the primitive polynomials stored in the primitive polynomial memory means according to the identification information extracted by the communication means and supplies coefficients of the primitive polynomial serving as the first coefficients to the first linear feedback shift register.

Brief Description of Drawings

[0012]

[Fig.1] Figure 1 is a functional diagram showing a pseudorandom number generator according to a first embodiment.

[Fig.2] Figure 2 is a circuit diagram showing a first linear feedback shift register.

[Fig.3] Figure 3 is a circuit diagram showing a second linear feedback shift register.

[Fig.4] Figure 4 is a flowchart showing a pseudorandom generation process according to the first embodiment.

[Fig.5] Figure 5 is a view showing changes in values of the first and second linear feedback shift registers.

[Fig.6] Figure 6 is a functional diagram showing a pseudorandom number generator according to a second embodiment.

[Fig.7] Figure 7 is a flowchart showing a

pseudorandom number generation process according to the second embodiment.

5